

Sub  
a1

ABSTRACT

The present invention provides a system and method for providing certified voice and/or multimedia mail messages in a broadband signed communication system which  
5 uses packetized digital information. Cryptography is used to authenticate the saved message using a certificate of the originators identity and electronic signature. A broadband communication system user may be provisioned for certified voice and/or multimedia mail by registering with a certified mail service provider and thereby receiving certification. The registration process may include the system user's customer  
10 premises equipment providing a cryptographic public key to the service provider. In response, the service provider issues a digital certificate certifying authenticity of the system user's identity and public key. Once the broadband communication system user has registered with a service provider for certified voice and/or multimedia mail and received the certificate, they may offer certified voice and multimedia mail to a calling  
15 party. When a caller communicates with a system user that is registered for certified mail, by for example making a telephone or multimedia call, he may be given the option of leaving a certified voice mail or certified multimedia mail. The caller and the called system user's customer premises equipment may keep track of the information packets used in the call. The called system user's CPE may then electronically sign the bits in  
20 the communication packets and return the message with an electronic signature of the called system user to the calling party, along with the system user's certificate obtained from the service provider / certifying authority during registration. The electronic signature is a cryptographic key of the called party. The calling party may then use its copy of the message, a copy of the message including the electronic signature received

25 from the called party, and the certificate, to undeniably prove to anyone in possession of the service provider's public key, that he left the voice or multimedia mail message for the called party. Further, the caller may prove that the call happened and that the message left was what he claims it to be by submitting this information to a judging authority.

30